(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 990 748 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.11.2008 Bulletin 2008/46

(51) Int Cl.:
G06F 19/00 *(2006.01)*

(21) Application number: **07107865.3**

(22) Date of filing: **09.05.2007**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK RS

(71) Applicant: **Golden Hour Data Systems, Inc.**
San Diego CA 92121 (US)

(72) Inventors:
- **Hutton, Kevin C**
  Solana Beach, CA 92075 (US)
- **Jones, Scott J**
  Escondido, CA 92026 (US)
- **Polany, Rany**
  Escondido, CA 92026 (US)

(74) Representative: **Flutter, Paula et al**
EIP
Fairfax House
15 Fulwood Place
London WC1V 6HU (GB)

(54) Integrated emergency medical transportation database and secure network system

(57) A system and method for providing secure data communications and user access authorization for an integrated emergency medical transportation database (12). The secure communications and user authorization may be provided, for example, by a Virtual Private Network ("VPN") (220), as well as alternate methods and systems described herein, allowing confidential patient medical records to be transmitted via a public network (50) such as the Internet without compromising the confidentiality of the data.

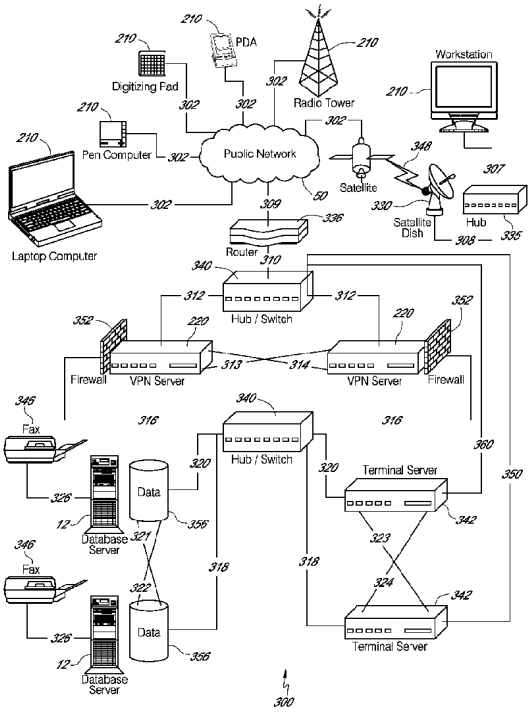

FIG. 3

EP 1 990 748 A1

Description

Field of the Invention

[0001] This invention relates to an integrated medical database system. More specifically, this invention relates to providing secure communications and user authorization for a medical database in the emergency medical transportation industry.

Description of the Related Technology

[0002] Current documentation procedures in the air medical transport industry are based on an inefficient paper and pencil technology. Important information is frequently collected on loose sheets of paper. In the environment of emergency medical transport, little time is available to neatly chart and document all pertinent and required information on a single document. Dispatch data, demographic data and clinical data are normally tracked as fragmented pieces of information, which are later coalesced into a complete patient chart. In many cases, these data include the same information, thus forcing the input of redundant information. The resultant chart is therefore vulnerable to being incomplete and unreliable. In a medical setting, incomplete information can lead to disastrous clinical results.

[0003] This same technology is used to support industry quality improvement and billing procedures and submit letters of transport justification. This paperwork is usually carried out at a later date, prolonging account receivable times in many instances to the point of compromising and jeopardizing service compensation. Inventory stocking and tracking is similarly a victim of extended turnover times and is often incomplete and inaccurate.

[0004] The fragmentation throughout the medical transport environment is also evident in the myriad of entities throughout the country practicing different standards of care and documentation. As is the case in other segments of the healthcare industry, even seemingly simple tasks of communicating among the various entities, as well as among sections of a single providing entity, is severely hampered by the lack of a common communication format. This is especially evident when certain aspects of the system (such as computerized clinical laboratory result displays) have been upgraded with a uniquely tailored computerized system, while the remaining functions are still performed in an archaic manner. While the upgraded system may be effective for one singular aspect, such as dispatching, lab reporting, or chart dictating, the remainder of the system does not improve its effectiveness due to the other archaic components.

[0005] In addition, current air medical transport services often transfer data in unsecure protocols and over unsecure public communication paths, and do not always validate users as being authorized users. Thus, current systems are susceptible to unauthorized users gaining access to the system and thereby compromising the integrity and confidentiality of the stored data, as well as the interception or corruption of data in transit via public communications networks, for example the Internet.

[0006] Therefore, a comprehensive system exists that includes modules for dispatching emergency medical teams, tracking their movement to and from the accident scene, managing a clinical diagnosis and treatment and accurately billing the patient for the services rendered. Such a system should optionally incorporate security and user authorization measures to ensure the integrity and confidentiality of the data that is transferred over public communications networks and data that is stored by the system. The system should also comply with applicable governmental regulations and guidelines, for example the European Standards on Confidentiality and Privacy in Healthcare (this Guidance was published in 2006), and future versions of these or other regulations.

Summary of Certain Inventive Aspects

[0007] In one aspect, a secure integrated emergency medical transportation database system includes a medical emergency database including at least clinical encounter information, patient demographic data and transport information as electronic protected health information, a billing module configured to access the medical emergency database and generate a bill for each medical emergency requiring transport, and a secure communications application configured to allow secure access to the medical emergency database and/or billing module by a plurality of authorized users via a public network, wherein the secure access comprises technical security measures to protect against unauthorized access to the electronic protected health information during transmission over the public network so that data indicative of a medical emergency is securely stored in the medical emergency database from a location in the field that is remote from a health service facility.

[0008] Further embodiments of the system may include the following features. The secure communications application may be additionally configured to allow the secure transfer of medical data via the public network. The secure access may be compliant with the European Standards on Confidentiality and Privacy in Healthcare. The secure access may protect against a risk of interception during electronic transmission of the health information. The secure access may be compliant with European Union patient privacy standards. The secure communications application may secure communications via the public network. The secure communications application may use secure sockets layer. The secure communications application may include a virtual private network. The secure communications application may include encryption and decryption algorithms. The secure communications application may include encryption and decryption keys. The secure communications application may authenticate validity of a one of the plurality of authorized users. The secure communications appli-

cation may include a dedicated, secure and encrypted channel. The transport information may include information obtained about the transport after first contact by medical transport personnel. The transport information may be associated with the clinical encounter information by at least patient pickup data. The system may additionally a portable computing device used by emergency medical personnel to wirelessly access a public network in real time while at the patient pick-up location or during a transport of an emergency medical services patient, and in further embodiments the secure communication application may be associated with the computing device, and the portable computing device may be used by emergency medical personnel inside an emergency transport vehicle. The transport information may include vehicle tracking information including segmental flight time for each transport segment. The technical security measures may minimize access to inappropriate information based on job requirements. The field location may be at a location between two health service facilities that are the source and destination of the transport.

[0009] In another aspect, a method of providing access to a secure integrated emergency medical transportation database system includes collecting at least clinical encounter information, patient demographic data and transport information as electronic protected health information for each of a plurality of medical emergency incidents requiring transport into a medical emergency database, accessing the medical emergency database, generating a bill for each medical emergency incident accessed, and securing access to the medical emergency database and/or billing information by a plurality of authorized users via a public network, where securing access comprises using technical security measures to protect against unauthorized access to electronic protected health information during transmission over the public network so that data indicative of a medical emergency is securely stored in the medical emergency database from a location in the field that is remote from a health service facility.

[0010] Further embodiments of the method may include the following features. The method may also include securing the transfer of medical data via the public network. Securing access may be compliant with the European Standards on Confidentiality and Privacy in Healthcare. Securing access may include protecting against a risk of interception during electronic transmission of the health information. Securing access may be compliant with European Union patient privacy standards. Securing access may include securing communications via the public network. Securing access may include using secure sockets layer. Securing access may include using a virtual private network. Securing access may include using encryption and decryption algorithms. Securing access may include using encryption and decryption keys. Securing access may include authenticating validity of a one of the plurality of authorized users. Securing access may include using a dedicated, secure and encrypted channel. The transport information may include patient pickup data and secmental flight time, and may be used for billing. The collecting may include wirelessly collecting the electronic protected health information by emergency medical personnel via a public network while at the scene of the patient encounter or during transport of an emergency medical services patient, and the wirelessly collecting may include using a portable computing device inside an emergency transport vehicle. The transport information may include vehicle tracking information including segmental flight time for each transport segment. The field location may be at a location between two health service facilities that are the source and destination of the transport.

Brief Description of the Drawings

[0011] The above and other aspects, features and advantages of the invention will be better understood by referring to the following detailed description, which should be read in conjunction with the accompanying drawings. These drawings and the associated description are provided to illustrate certain embodiments of the invention, and not to limit the scope of the invention.

[0012] Figure 1 is a diagram of an on-line computing environment of a medical database system in which a Virtual Private Network ("VPN") may operate in accordance with one embodiment of the present invention.

[0013] Figure 2 is a diagram of top-level VPN system components in accordance with one embodiment of the medical database system of Figure 1.

[0014] Figure 3 is a diagram of detailed VPN system components in accordance with the medical database system embodiment of Figures 1 and 2.

[0015] Figure 4 is a block diagram of client applications of the user device, VPN server, and terminal server components as shown in the embodiment of Figure 3.

[0016] Figure 5 is a flowchart of database access operations of the medical database system in accordance with the embodiments of Figures 1-3.

[0017] Figure 6 is a diagram of one example of a database configuration layout in accordance with one embodiment of the medical database system.

Detailed Description of Certain Embodiments

[0018] The following detailed description of certain embodiments presents various descriptions of specific embodiments of the present invention. However, the present invention can be embodied in a multitude of different ways as defined and covered by the claims. In this description, reference is made to the drawings wherein like parts are designated with like numerals throughout.

[0019] In certain embodiments, the present invention relates to an object oriented, interactive, international, client-server service for the medical transport industry. The service may integrate all aspects of patient record documentation into a single complete electronic chart. A

server computer provides chart database information access to multiple transport providers simultaneously by securely transmitting, storing and maintaining standardized patient data, for instance, using guidelines set forth by the Scrambling Standards Organization. Individual transport-providing entities, such as helicopter and ambulance companies, obtain coded access to this server via phone lines with a modem-equipped personal computer. Security is maintained by assigning each entity a unique code or identifier. Integrated Services Digital Network ("ISDN") lines, Digital Satellite Systems ("DSS"), dedicated trunk lines (for example T1, T3), cable modems, digital subscriber lines ("DSL"), or digital wireless systems may also be used for communication. Such an emergency medical transportation database system is described in U.S. Patent No. 6,117,073, which is hereby incorporated by reference in its entirety.

[0020] Each crew member involved in the patient's chart documentation, i.e. dispatcher, flight nurse, paramedic and physician, as well as administrator and collector, possess coded access to chart portions relevant to their responsibilities and level of care provided. The chart is then electronically generated from the compendium of the information entered in a standardized fashion and in accordance with minimum industry documentation requirements and the inventory of financial health care standards. The system provides complete and accurate chart documentation and maintains internal consistency between each separate module. Furthermore, any sentinel events are automatically referred to the appropriate, responsible party. A sentinel event is any action during the encounter that might require a further review. Examples of sentinel events are scene times exceeding 40 minutes, nonsensical data entry by an emergency transport crew member, supply shortages for equipment not utilized or repeated claim denials.

[0021] Billing can be submitted electronically to the appropriate party in an appropriate format that reduces the accounts receivable times for each patient encounter. Letters of justification are automatically generated as well as follow up letters and utilization review reports. Inventory reports and lists of necessary base supplies and medicines are also electronically updated to appropriate supply centers and administrators. Customized and research reports can also be provided rapidly.

[0022] Data security and an automatic backup are provided. Although the chart data is normally made the property of the respective transport service provider, the system can retain non-proprietary data to provide industry benchmarking, quality assurance analysis and clinical research opportunities. Such standardized data collection and documentation will furthermore enable the development of an Emergency Medical Services data library to assist in the justification and legislation of governmental preventive policies for public safety.

[0023] The communication of data via a public network would normally be susceptible to being intercepted by unauthorized users. In the medical transportation system, data communicated via the public network may include confidential information such as patient medical records. The present invention includes a Virtual Private Network ("VPN") operating on the public network to ensure confidentiality of the patient data. A system according to the present invention complies with applicable regulations regarding the confidentiality of patient data, for example the European Standards on Confidentiality and Privacy in Healthcare, or other European Union patient privacy standards. The VPN of the emergency medical transportation system may be thought of in terms of a three-tier architecture: 1) the user, 2) the business rules processing, and 3) the database.

[0024] Figure 1 provides an overview of the computer hardware involved in one embodiment of a medical database system 100. In this embodiment, the medical database system 100 includes a server computer 12. The server computer 12 can be based on many microprocessors, such as those manufactured by Intel, Motorola, IBM or other chip manufacturers. The server computer 12 enables rapid simultaneous access to many users of the system. In one embodiment, the server computer 12 is an Intel Pentium III class computer having at least 256 Megabytes of RAM and a 10 gigabyte hard disk drive and a 500 megahertz ("MHz") processing speed. In addition, many other standard or non-standard computers may support various embodiments of the medical database system 100.

[0025] The database application may be programmed in, for instance, ACIUS's 4th Dimension language and used in conjunction with the 4D Server and Client program. Also, another alternative computer environment is Microsoft Corporation's Visual Basic language with C++ middleware and the BackOffice SQL Server program. It can therefore run in a standard Windows/Macintosh point-and-click office environment, and requires no additional specialized software programming by the user. Additionally, other standard or non-standard computing environments may support embodiments of the medical database system 100.

[0026] As illustrated in the embodiment of Figure 1, the server computer can access a chart database 13. The chart database 13 stores the previously described electronic charts corresponding to patients that have utilized emergency medical transportation. The server computer can also access a statistical database 14 to store and extract statistical information from data entered during patient encounters. The collected statistics might include, for example, average scene and transport times, number of transport requests per demographic region and time of year, average number of advanced procedures performed by crew members and number of complications encountered. In addition, the database 14 can hold information relating to the average length of time to process claims by category and payment plan.

[0027] The server computer 12 can also be linked to a regional trauma database 15. The database 15 stores information relating to, for example, local trauma centers,

emergency medical practice, and other local trauma-related information.

[0028] The dispatch module on the server computer 12 can be accessed via an interface to a dispatch computer 20, which might reside, for example, at the dispatch center that receives the initial call to deploy an emergency medical team. The dispatch computer 20 may provide a communications interface to the server computer 12 so that it acts as computer terminal, or it may contain a portion of the dispatch module.

[0029] Based on the scene location and needs of the patient, the dispatch center might deploy, for example, a helicopter 24, airplane 25 or ambulance 26. The dispatch computer 20 communicates with software applications for collecting information on the patient encounter and scheduling and deploying a crew to assist the injured patient. Within one embodiment of the medical database system 100, the helicopter 24, airplane 25 or ambulance 26 would include a portable computing device ("user device") 210 that is used by the emergency medical team during the patient encounter. A wireless connection 32 can be made by the user device 210 to the server computer 12, via a public network 50, for example the Internet, a Wide Area Network (WAN), or an Intranet, to update the database 14 after data is entered. The user device 210 may include clinical and diagnosis modules to assist the emergency medical team in treating the injured patient, or may act as a terminal device to communicate with these modules on the server computer 12. The clinical and diagnosis modules assist the emergency medical team in determining the proper diagnosis and treatment of the patient.

[0030] One embodiment of the medical database system 100 may also include a billing computer 36 in communication with the server computer 12 via a public network 50, for example the Internet. The billing computer 36 interfaces with the server computer 12 to run the billing module for tracking inventory. The billing module can be stored directly on the billing computer 36 or, alternatively, stored on the server computer 12 and accessed via the billing computer 36 over the public network 50. The billing module may be used to track inventory and medical equipment. In addition, it may be used during the patient encounter for providing billing functions within the medical database system 100. The billing computer 36 may additionally communicate with a printing device 38, for example an inkjet printer, laser printer, dot matrix printer, or other printing device, to provide printed reports and bills to hospitals, patients and medical centers.

[0031] An administration computer 40 communicates with the server computer 12 via the public network 50 to provide administrative reports. These reports relate to the statistical information stored in the statistical database 14. In addition, the administration computer 40 can run reports that relate to payroll, inventory, flight training, or many other administrative issues.

[0032] It should be noted that the dispatch computer 20, user device 210, and billing computer 36 can communicate with the server computer 12 through a variety of communications modes and protocols. For example, a wireless Local Area Network ("LAN") or cellular network may connect the various computers with one another. In another embodiment, dedicated or dial-up phone lines may be used to communicate between the different computers.

[0033] Figure 2 is a diagram of top-level VPN system components 200 in accordance with one embodiment of the medical database system 100 of Figure 1. As described in further detail below in relation to Figure 3, the user device 210 may consist of one or more types of portable computing device configured to communicate via various communications modes and protocols. In the embodiment of Figure 2, the user device 210 is configured to communicate over a public network 50, one example being the Internet. The public network 50 enables the user device 210 to communicate with one or more VPN server 220 for logging in and accessing the one or more database servers 12 of the medical database system 100. The logging in and accessing of the database servers 12 is described in further detail below in relation to Figure 3.

[0034] As used herein, the VPN server 220 enables a secure and encrypted communications link between certain nodes on the public network 50. While the nodes can communicate with each other, it is virtually impossible for other nodes to decipher the meaning of the signals or send signals that are believed to be authentic. One secure communications technology that facilitates such a VPN is Secure Sockets Layer ("SSL"). Other secure communications technologies may be used as well, and although SSL is a transport protocol, other security techniques that are not transport protocols may be utilized. The non-SSL techniques may be such that it will quickly and efficiently encrypt and likewise decrypt the data that is being transmitted via the public network 32. Thus, data security and user authentication does not require an expensive and geographically limited dedicated private network, but may be accomplished utilizing VPN technology via a public network 50 such as the Internet.

[0035] A VPN server refers to software, hardware, or both that secure network communications and authenticate validity of users in such a way as to minimize the possibility that it can altered or inappropriately viewed or transmitted. A VPN can operate between a number of internet-enabled devices. For example, a VPN can run on two or more computers that are connected together using security technologies such as SSL. In another embodiment, a VPN can operate between a client computer and a server computer using security technologies. In yet another embodiment, a VPN can additionally operate between many client computers and/or many server computers. Many types of portable devices can be used as user devices 210 as part of the VPN as well, as described in further detail below in relation to Figure 3.

[0036] Figure 3 is a diagram of detailed VPN system components 300 in accordance with the medical data-

base system 100 embodiment of Figures 1 and 2. As shown in Figure 3, many user devices 210 and modes of data communication 302 may be used to transfer data from the transporting vehicle (see part numbers 24, 25 and 26 in Figure 1) to/from the medical database system 100 via the public network 50. A non-exhaustive list of user devices 210 that may be used include a laptop computer, a pen computer, a digitizing pad, a personal digital assistant ("PDA"), a wireless device communicating via radio frequency ("RF") waves with a radio tower or a satellite, or a computer communicating with a satellite via a hub 335 and a satellite dish 330.

[0037] In the embodiment of Figure 3, the user devices 210 may communicate via the public network 50 utilizing a number of various modes and protocols of communication 302. For example, such modes of communication 302 include a Universal Serial Bus ("USB"), Firewire, Infrared signals, Bluetooth wireless communications, IEEE 802.2 signals, radio frequency signals such as those of frequency 900 megahertz or higher, straight-through and crossover Ethernet cables, switched packets or sockets transmission, token rings, frame relays, T-1 lines, DS connections, fiber optic connections, RJ-45 and RJ-11 connections, serial pin connections, ultrasonic frequency connections, and satellite communications. Other modes and protocols of communication 302 are also possible and are within the scope of the present invention.

[0038] In one embodiment, the user device 210 communicates via the public network 50 with a network communications routing device ("router") 336, for example a main gateway router, which directs network traffic between the appropriate network servers. Examples of commercially available network routers 336 include those made by Cisco, Linksys, Netgear, Netopia, and Hewlett-Packard. The data communications from the user device 210 are directed by the router 336 to the medical database system 100 via a network hub or switch 340. The hub or switch 340 forwards the data communication packets to one or more VPN server 220.

[0039] Current technologies that offer VPN server 220 capabilities include hardware, software, and a combination of hardware and software that function both independently and together with other VPN servers 220. In the embodiment of Figure 3, two VPN servers 220 or shown as an example, but other embodiments may include one VPN server 220, while still other embodiments may include more than two VPN servers 220. Vendors may package VPN capabilities into a device termed an "appliance," which is typically a dedicated hardware device configured with embedded security policies. VPN vendors and manufacturers include, for example, Nortel, Checkpoint, Nokia, Sun Microsystems, Cisco, Netopia, Compaq, IBM, Hewlett-Packard, Watchguard, Linksys, Netgear, and Lucent. Such VPN systems provide system administrators the ability to set security policies and rules as to the rights each user and each application will be allowed on the servers of the medical database system.

[0040] In one embodiment, the VPN servers 220 provide encryption and decryption keys to a user, so that the user's data communications are secured using various encryption/decryption algorithms, including, for example, DES, 3DES, MD5, SHA, 40-bit, 56-bit, 128-bit, 168-bit, and other types of encryption/decryption algorithms. In this way, the user establishes a secure communication to the servers of the medical database system 100, using one or a redundant array of VPN servers 352. Further, to increase system up time and reliability, a failsafe protocol can be implemented to achieve a fail over configuration by connecting redundant communications 313, 314. In such a configuration of VPN servers 352, if one VPN server 352 fails, one or more of the other VPN servers 352 undertakes the workload, so that the user is likely not even aware that a failure has occurred.

[0041] One or more firewalls 352 may be configured in order to secure the connection beyond the router 336 by preventing external network access to the servers comprising the medical database system 100 by non-authorized devices and/or users on the public network 50. The firewalls 352 may be a separate hardware device, or may be either hardware and/or software that is incorporated into the VPN servers 220. The VPN servers 220 authenticate the users that login to the medical database system 100 and allow only those authorized users access to the medical database system 100 servers through the firewalls 352.

[0042] Data communications that the firewalls 352 in conjunction with the VPN server 220 allow to pass through to the servers of the medical database system 100 are forwarded by a hub or switch device 340 to either a terminal server 342 or to a database server 12. The embodiment of Figure 3 shows two terminal servers 342 and two database server 12, but more or fewer terminal servers 342 and more or fewer database servers 12 may also be used in further embodiments. In addition, the number of terminal servers 342 may be different than the number of database servers 12 in certain embodiments. The terminal servers 342 and/or database servers 12 may be configured as a server farm. A server farm refers to a pool or multitude of servers functioning together to perform common server functionality. In one embodiment, an authorized user may initiate two types of connections to the medical database system 100, a terminal server request or a direct database server request. Such server farms are able to perform load balancing or failsafe switching of servers should one or more become non-operational to accomplish redundancy or system efficiency.

[0043] In one embodiment, a direct database server request may be made by the user to connect the user device 210 to the database server 12. The database 356 and database server 12 operate in a client/server relationship, such that in order to access the database, the user establishes a client connection to the database server 12. Database 356 access is accomplished by making database requests to the database server 12 over a secure, password protected, and dedicated channel of

communication. In cases where the communications channel supports a direct connection, i.e. low communications latency, sufficient data communication bandwidth, or strong system configuration, the user devices 210 can communicate directly with the database servers 12.

[0044] The database 356 and database server 12 contain the operating system components to run the core system, for example, Macintosh, Windows, Linux, Unix, and other operating systems. In one embodiment of the medical database system 100, the database server 12 and database 356 utilize a database that is ODBC, Sequel, Sybase, 4D, and Oracle compliant such that it can integrate with a majority of these operating systems and other database systems. The data may be stored on a main database server 12, but may also be configured to mirror and fail-safe over to another database system, achieving redundancy, system efficiency, and backup efficiency, among other benefits.

[0045] Current database 356 technologies include commercially available brand and product names, for example, Oracle, 4D, Sequel Server, Sybase, Filemaker, Access, Cold Fusion, FoxPro, and other database systems. Such databases function as relational databases that allow for querying and database development on multiple planes, and also for granting user specific access to regions of the database. These databases also typically include client software applications that communicate with the database 356. The client software applications are installed on the user workstation and create a channel of communication with the user and the database 356.

[0046] However, in other cases, the communications channel does not support a direct connection, so the user device 210 communicates with the database servers 12 through the terminal servers 342. A terminal server request may be made by the user to connect the user device 210 to the terminal server 342, such that the terminal servers 342 deliver a screen to the user to control a remote server. The terminal servers 342 allow multiple users to connect to run a heterogeneous portfolio of applications, providing the user with what appears to be a personal and individual work session. Thus, the user may remotely control the terminal servers 342 to perform the communications processing with the database servers 12 as described above. The terminal server 342 may be many various types of devices running various types of operating systems, for example Microsoft servers, Unix servers, BSD, Apple Macintosh, Linux, and other computer systems and operating systems. Some examples of common enterprise level software platforms in current existence and use include, for example, Microsoft Terminal Services using the Remote Desktop Protocol ("RDP"), Cisco PIX Firewalls, PCAnywhere, Timbuktu, VNC, and Citrix Metaframe software applications. In a further embodiment, a fax machine 346 may optionally be connected to the database servers 356, enabling the database servers 356 to send faxes, for example, when a paper invoice is required to be sent.

[0047] Figure 4 is a block diagram of client applications of the user device 210, VPN server 220, and terminal server 342 components as shown in the embodiment of Figure 3. In this embodiment, the user devices 210 include client applications for the terminal server user application 410 and database client application 416. As described above in relation to Figure 3 and below in relation to Figure 5, one embodiment of the user devices 210 only includes one or the other of the terminal server user application 410 and database client application 416, depending on whether the user connects to the database servers 12 directly or connects through the terminal servers 342. However, other embodiments may include both of these applications 410, 416. In one embodiment, the database client application 416 is the Citrix client Metaframe, or it may additionally be Nfuse, which allows the use of a web browser.

[0048] The user devices 210 additionally include operating system software 420, for example Macintosh, Windows, Linux, Unix, or other computer operating systems. The user devices 210 may additionally include a browser application 426 for accessing the public network 50 such as the Internet and allowing the display of and interaction with various websites accessible via the Internet. For example, several such commonly used browser applications are Microsoft Internet Explorer and Netscape Navigator.

[0049] In the embodiment of Figure 4, the VPN servers 220 include client applications for the firewall 436 and VPN applications 440, which may both be provided by a single application, for example Checkpoint VPN1. The VPN application 440 utilizes encryption keys 430 and is controlled by policies and privileges 456 that are set up by someone with system administrator level privileges. For example, the policies and privileges 456 include specifying which ports are authorized to send data in what direction (e.g. input, output, or both), and specifying which applications are authorized to access which ports. The VPN servers 220 additionally include operating system software 446, as described above in relation to the user device 210 of Figure 4. The VPN servers 220 additionally include Local Area Network ("LAN") application software, for example TCP/IP, UDP, IPS/SPX, NetBeui, NetBios, XML, and AppleTalk, for file sharing, printing, internal server communications, and other LAN network capabilities.

[0050] In one embodiment, the terminal servers 342 include the database client application 416 as described above in relation to the user device 210 of Figure 4. The terminal servers 342 additionally include a terminal server application 470, an operating system software 476 as described above in relation to the user device 210 of Figure 4, and the LAN application 460 as described above in relation to the VPN server 220 of Figure 4.

[0051] While the embodiment of Figure 4 shows a specific example of the client applications that may be included in the user devices 210, VPN servers 220, and

terminal servers 342, other embodiments utilizing other client applications in various configurations are also within the scope of the present invention. As Figure 4 illustrates one embodiment of the devices and servers of the medical database system 100, the present invention is not limited to this embodiment but also includes other embodiments as well.

[0052] Figure 5 is a flowchart of database access operations of the medical database system 100 in accordance with the embodiments of Figures 1-3. At stage 510, the user initiates the login connection for a VPN client key. At stage 516, the VPN client key request is tagged and encapsulated with information and sent for authentication within the VPN server 220. The VPN server 220 includes a decision process mechanism for funneling applications and users to the predetermined authorized areas within the public network 50. The VPN server 220 additionally blocks those activities that are not authorized within the policies as set by the system administrator. Another function of the VPN server 220 is to make the user authentication determination shown at stage 520. At decision stage 526, the system either allows successful access to the database system, or denies access to the requesting user. Upon such a denial of access, at stage 530 the system administrator is optionally notified of the denial of access to the user. The system may utilize a variety of ways of notifying the system administrator, such as via paging, fax, email, audio/visual alerts, entry into a log file, or other ways of notification. The user may attempt the login and authentication process again at stage 510.

[0053] If the user authentication at stage 526 is instead successful, the user is notified of successful VPN access. A notification may additionally be sent to the system administrator, for example, via email, fax, audio/visual alerts, log file entry, or other notification means. At stage 536, the user logs in to the VPN server 220 and further communications utilize a dedicated, secure, and encrypted channel. Private VPN level connections are designed and configured with a high level of security and encryption to maintain data confidentiality. The VPN encapsulates the data and creates encryption around each packet of information with a variety of different encryption schemes that are enforced by the database server 12 and the database 356. In the current technology, standard encryption uses 40 bit, 56 bit, 128 bit, and 168 bit keys. Trends in the technology indicate that in the future these degrees of encryption will be enhanced, or may possibly use a combination of levels to maximize efficiency and encoding.

[0054] At optional stage 540, the user may log in to the terminal server 342 to communicate with the database server 12 via the terminal server 342. However, at stage 546 the user may also elect to log in directly to the database server 12 and bypass the terminal server login at stage 540. Having logged in to the database server 12, the database server 12 determines, based on the authentication level, the access that the user will be allowed, which in turn governs which of the following operations the user may perform. At stage 550 the user may elect to perform administrator operations, assuming the user has the required authentication level. At stage 556 the user may elect to perform billing operations, again assuming the user has the required authentication level. At stage 560 the user may elect to perform clinical operations, assuming the user has the required authentication level. At stage 566 the user may elect to perform dispatch operations, once again assuming the user has the required authentication level. In other embodiments, the users may elect to perform other medical database system operations they are authorized to perform that are not shown in the embodiment of Figure 5.

[0055] At decision stage 570, the user may elect to log off the medical database system 100 and end the operations shown in Figure 5, or alternatively the user may elect to remain logged in to the system and elect another operation to perform.

[0056] Figure 6 is a diagram of one example of a database configuration layout 600 in accordance with an embodiment of the medical database system 100. In this embodiment, a medical database record, which may be stored in the chart database 13 shown in Figure 1, includes fields for medical condition 610, patient information 620, patient location 630, transportation destination 640, means of transportation 650, and estimated time of arrival ("ETA") 660. In other embodiments, the medical records may include more or fewer fields than are shown in the embodiment of Figure 6. In addition, the databases may include more or fewer record entries than shown in the embodiment of Figure 6.

[0057] The database configuration layout 600 example shown in Figure 6 may contain confidential patient medical information. Such database records are securely transferred between the database 356 and the various servers of the medical database system 100 as described above in relation to the VPN system in Figures 3 and 5. The patient information is essentially safe from interception by unauthorized users on the public network 50 in a system as described herein.

[0058] While the above detailed description has shown, described, and pointed out novel features of the invention as applied to various embodiments, it will be understood that various omissions, substitutions, and changes in the form and details of the device or process illustrated may be made by those skilled in the technology without departing from the spirit of the invention. The scope of the invention is indicated by the appended claims rather than by the foregoing description. All changes that come within the meaning and range of equivalency of the claims are to be embraced within their scope.

Claims

1. A secure integrated emergency medical transportation database system (100), comprising:

a medical emergency database (12) comprising at least clinical encounter information, patient demographic data and transport information as electronic protected health information;
a billing module (36) configured to access the medical emergency database and generate a bill for each medical emergency requiring transport; and
a secure communications application (440) configured to allow secure access to the medical emergency database and/or billing module by a plurality of authorized users via a public network (50), wherein the secure access comprises technical security measures to protect against unauthorized access to the electronic protected health information during transmission over the public network so that data indicative of a medical emergency is securely stored in the medical emergency database from a location in the field that is remote from a health service facility.

2. The system of Claim 1, wherein the secure communications application is additionally configured to allow the secure transfer of medical data via the public network.

3. The system of Claim 1, wherein the secure access is compliant with the European Standards on Confidentiality and Privacy in Healthcare.

4. The system of Claim 1, wherein the secure access protects against a risk of interception during electronic transmission of the health information.

5. The system of Claim 1, wherein the secure access is compliant with European Union patient privacy standards.

6. The system of Claim 1, wherein the secure communications application secures communications via the public network.

7. The system of Claim 1, wherein the secure communications application uses secure sockets layer.

8. The system of Claim 1, wherein the secure communications application includes a virtual private network (220).

9. The system of Claim 1, wherein the secure communications application includes encryption and decryption algorithms.

10. The system of Claim 1, wherein the secure communications application includes encryption and decryption keys (430).

11. The system of Claim 1, wherein the secure communications application authenticates validity of a one of the plurality of authorized users.

12. The system of Claim 1, wherein the secure communications application includes a dedicated, secure and encrypted channel.

13. The system of Claim 1, wherein the transport information comprises information obtained about the transport after first contact by medical transport personnel.

14. The system of Claim 1, wherein the transport information is associated with the clinical encounter information by at least patient pickup data.

15. The system of Claim 1, additionally comprising a portable computing device (210) used by emergency medical personnel to wirelessly access a public network in real time while at the patient pick-up location or during a transport of an emergency medical services patient.

16. The system of Claim 15, wherein the secure communication application is associated with the computing device.

17. The system of Claim 15, wherein the portable computing device is used by emergency medical personnel inside an emergency transport vehicle (24,25,26).

18. The system of Claim 1, wherein the transport information comprises vehicle tracking information including segmental flight time for each transport segment.

19. The system of Claim 1, wherein the technical security measures minimize access to inappropriate information based on job requirements.

20. The system of Claim 1, wherein the field location is at a location between two health service facilities that are the source and destination of the transport.

21. A method of providing access to a secure integrated emergency medical transportation database system (100), comprising:

collecting at least clinical encounter information, patient demographic data and transport information as electronic protected health information for each of a plurality of medical emergency incidents requiring transport into a medical emergency database (12);
accessing the medical emergency database;
generating a bill for each medical emergency incident accessed; and

securing access to the medical emergency database and/or billing information by a plurality of authorized users via a public network (50), wherein securing access comprises using technical security measures to protect against unauthorized access to electronic protected health information during transmission over the public network so that data indicative of a medical emergency is securely stored in the medical emergency database from a location in the field that is remote from a health service facility.

22. The method of Claim 20, further comprising securing the transfer of medical data via the public network.

23. The method of Claim 20, wherein securing access is compliant with the European Standards on Confidentiality and Privacy in Healthcare.

24. The method of Claim 21, wherein securing access comprises protecting against a risk of interception during electronic transmission of the health information.

25. The method of Claim 21, wherein securing access is compliant with European Union patient privacy standards.

26. The method of Claim 21, wherein securing access comprises securing communications via the public network.

27. The method of Claim 21, wherein securing access comprises using secure sockets layer.

28. The method of Claim 21, wherein securing access comprises using a virtual private network (220).

29. The method of Claim 21, wherein securing access includes using encryption and decryption algorithms.

30. The method of Claim 21, wherein securing access includes using encryption and decryption keys (430).

31. The method of Claim 21, wherein securing access includes authenticating validity of a one of the plurality of authorized users.

32. The method of Claim 21, wherein securing access comprises using a dedicated, secure and encrypted channel.

33. The method of Claim 21, wherein the transport information comprises patient pickup data and segmental flight time, and is used for billing.

34. The method of Claim 21, wherein the collecting comprises wirelessly collecting the electronic protected health information by emergency medical personnel via a public network while at the scene of the patient encounter or during transport of an emergency medical services patient.

35. The method of Claim 34, wherein the wirelessly collecting comprises using a portable computing device (210) inside an emergency transport vehicle (24,25,26).

36. The method of Claim 21, wherein the transport information comprises vehicle tracking information including segmental flight time for each transport segment.

37. The method of Claim 21, wherein the field location is at a location between two health service facilities that are the source and destination of the transport.

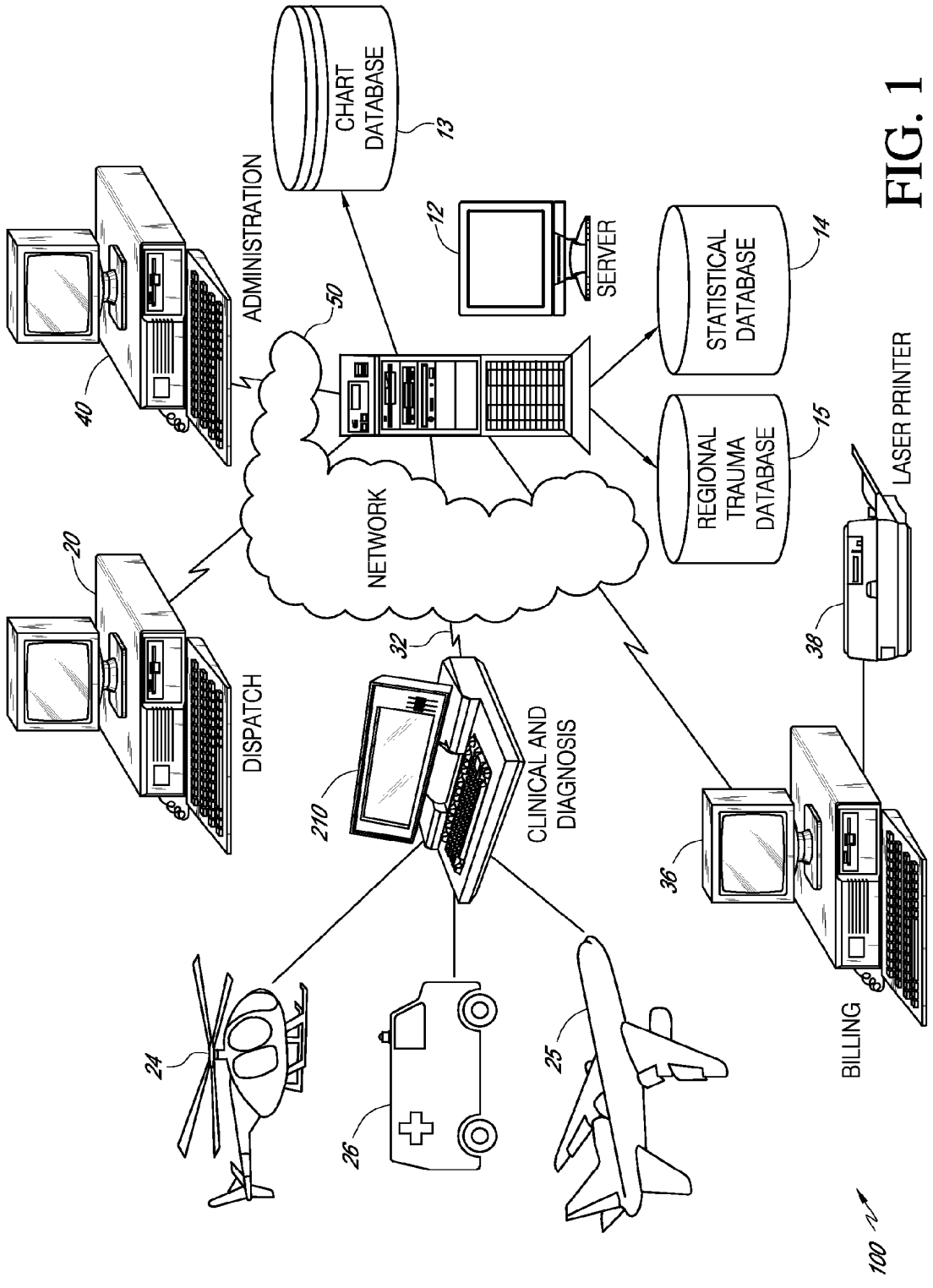
CHART DATABASE
13
ADMINISTRATION
40
50
12
SERVER
STATISTICAL DATABASE
14
REGIONAL TRAUMA DATABASE
15
LASER PRINTER
38
NETWORK
20
DISPATCH
32
210
CLINICAL AND DIAGNOSIS
36
BILLING
24
26
25
100

FIG. 1

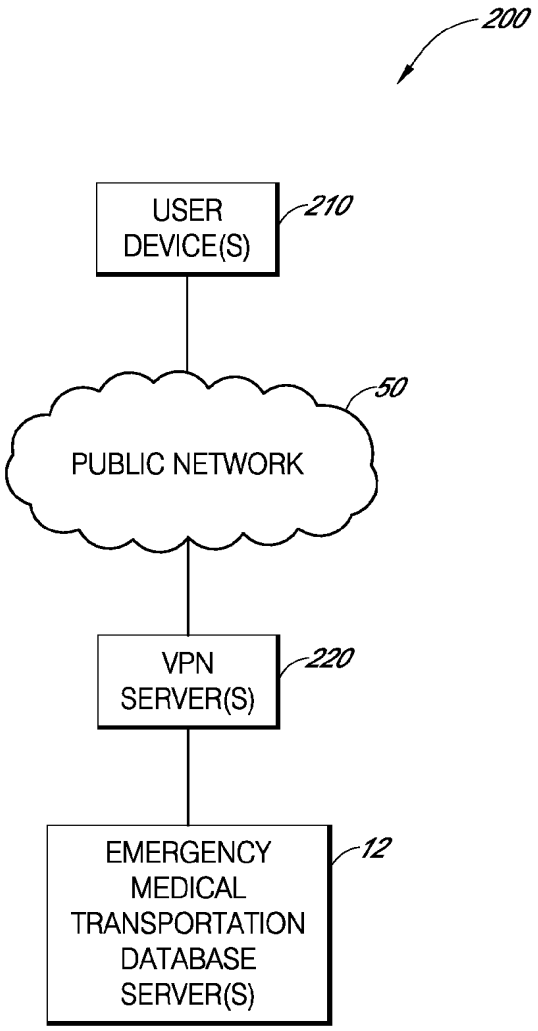
200
USER DEVICE(S)
210
PUBLIC NETWORK
50
VPN SERVER(S)
220
EMERGENCY MEDICAL TRANSPORTATION DATABASE SERVER(S)
12

FIG. 2

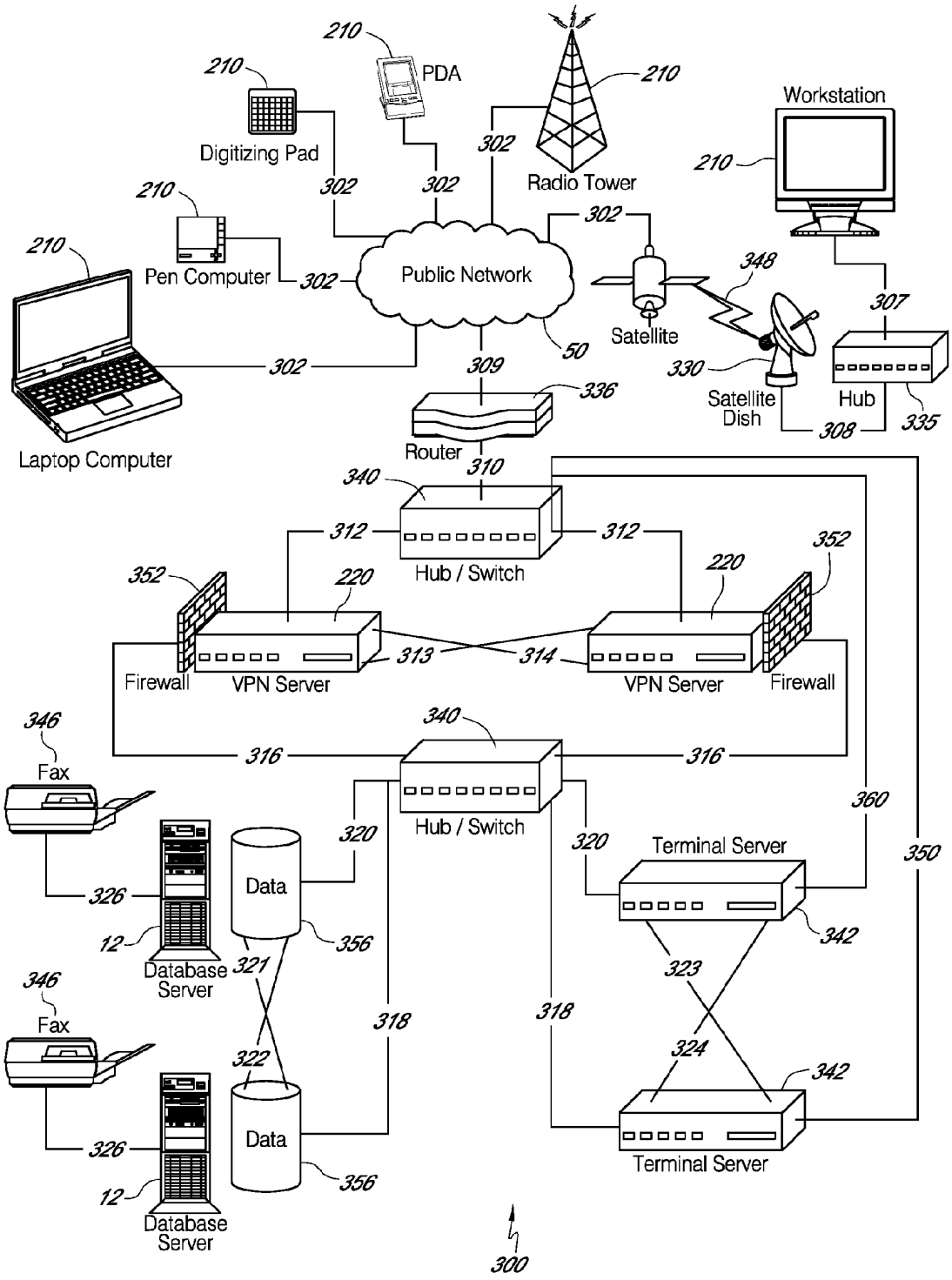
210
PDA
210
Digitizing Pad
210
Radio Tower
210
Workstation
210
Pen Computer
210
Laptop Computer
302
Public Network
50
Satellite
348
Satellite Dish
330
307
Hub
335
308
309
336
Router
310
340
Hub / Switch
312
352
220
Firewall
VPN Server
313
314
VPN Server
Firewall
316
346
Fax
320
Data
326
12
Database Server
321
356
322
318
360
350
Terminal Server
342
323
324
300

FIG. 3

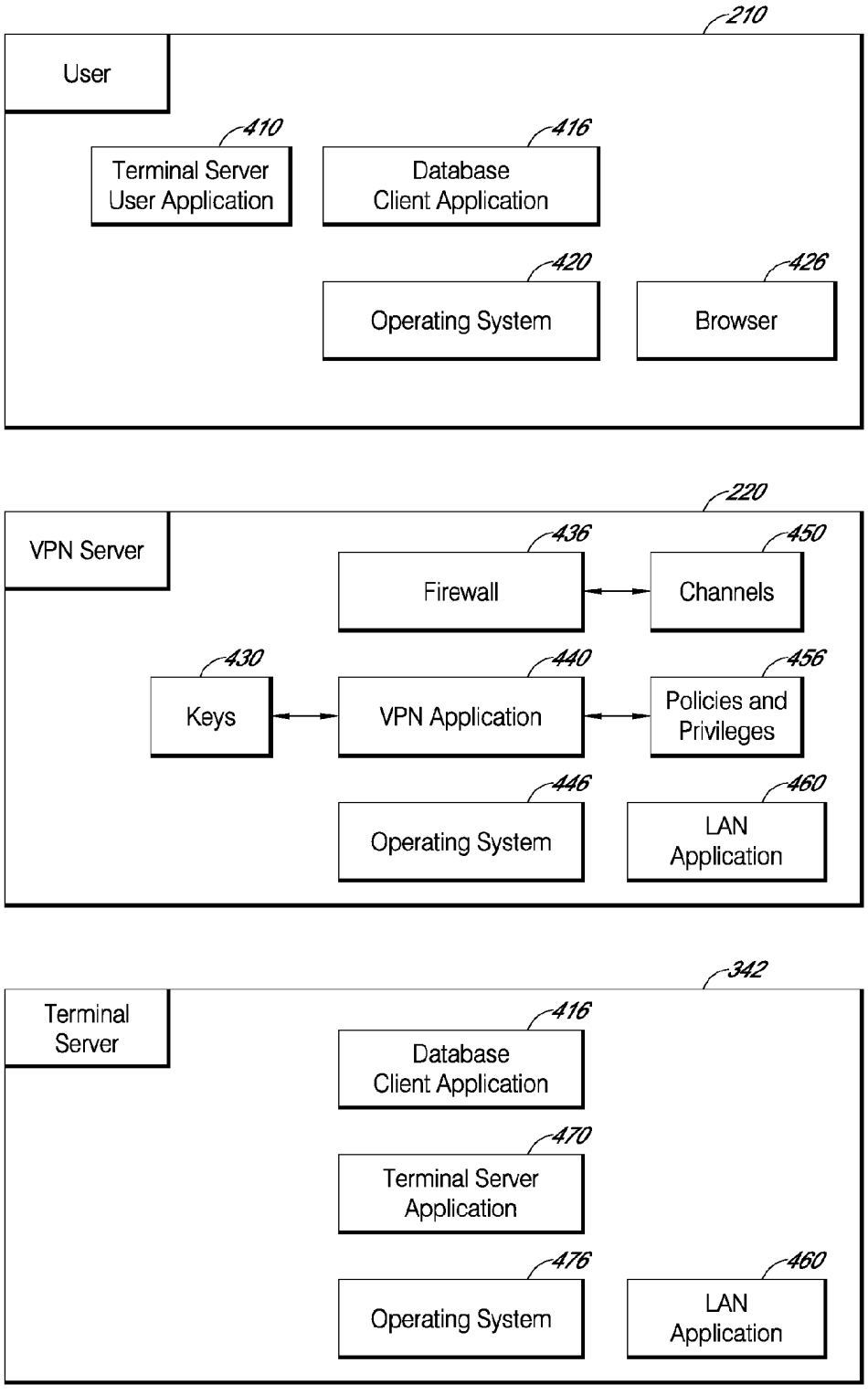
210
User
410
Terminal Server User Application
416
Database Client Application
420
Operating System
426
Browser
220
VPN Server
436
Firewall
450
Channels
430
Keys
440
VPN Application
456
Policies and Privileges
446
Operating System
460
LAN Application
342
Terminal Server
416
Database Client Application
470
Terminal Server Application
476
Operating System
460
LAN Application

FIG. 4

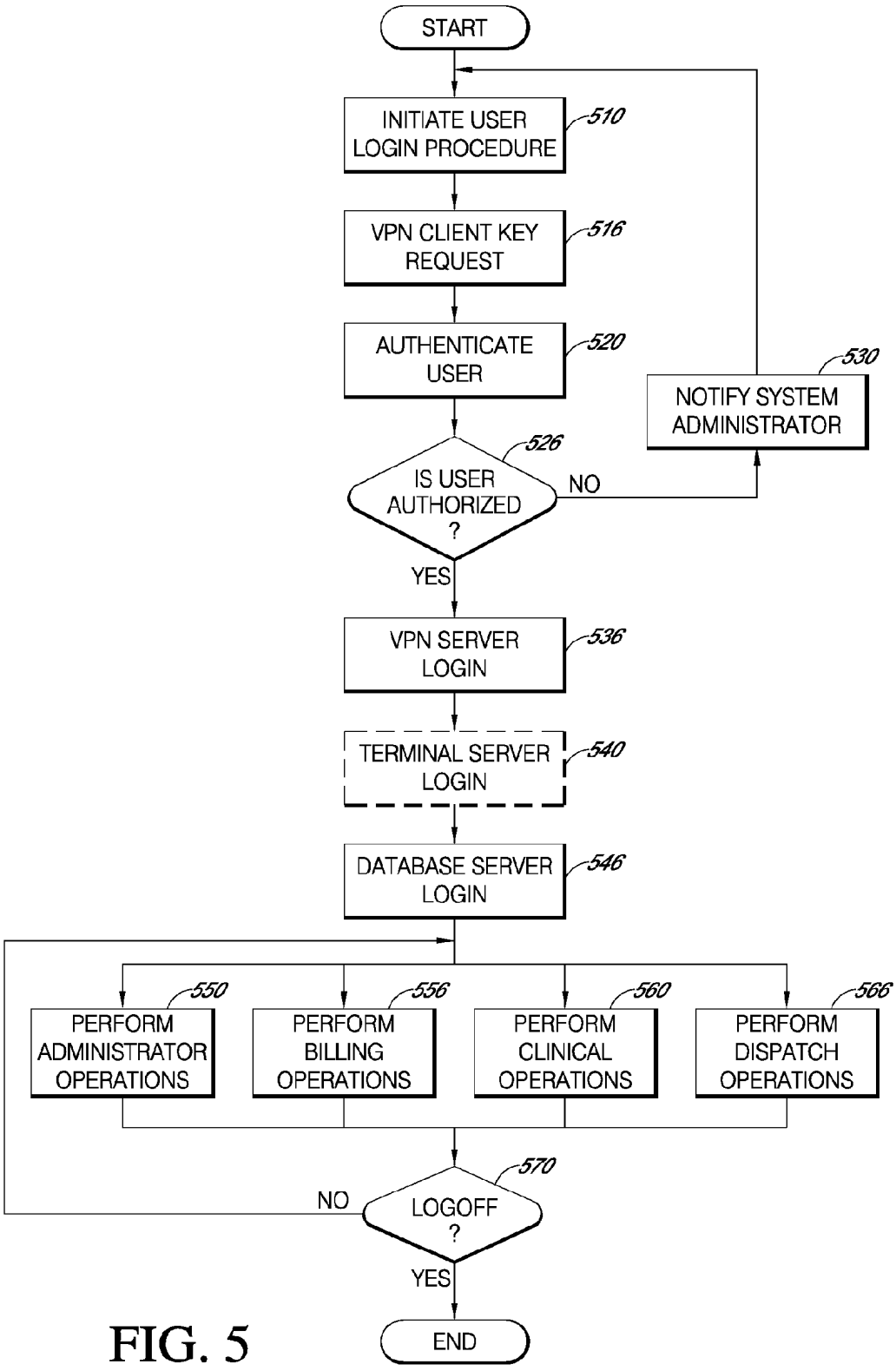
START
INITIATE USER LOGIN PROCEDURE
510
VPN CLIENT KEY REQUEST
516
AUTHENTICATE USER
520
NOTIFY SYSTEM ADMINISTRATOR
530
IS USER AUTHORIZED ?
526
NO
YES
VPN SERVER LOGIN
536
TERMINAL SERVER LOGIN
540
DATABASE SERVER LOGIN
546
PERFORM ADMINISTRATOR OPERATIONS
550
PERFORM BILLING OPERATIONS
556
PERFORM CLINICAL OPERATIONS
560
PERFORM DISPATCH OPERATIONS
566
LOGOFF ?
570
NO
YES
END

FIG. 5

610 Medical Condition	620 Patient Information	630 Patient Location	640 Transport To	650 Transportation Means	660 ETA
Apparent Heart Attack	Male, 70, home address, insurance info.	Rural City Hospital	Metro Medical Center	LifeFlight Airmedical	12:30 p.m.
Head Trauma	Female, 35, home address, insurance info.	Fashion Valley Mall	Memorial Hospital	Ambulance	1:53 p.m.
Internal Injuries	Male, 12, home address, insurance info.	123 Maple St. Anytown, USA.	Memorial Hospital	LifeFlight Airmedical	9:15 a.m.
....					

600

FIG. 6

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 07 10 7865

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X,D	US 6 117 073 A (JONES SCOTT J [US] ET AL) 12 September 2000 (2000-09-12) * the whole document *	1-37	INV. G06F19/00
X	US 2002/010679 A1 (FELSHER DAVID PAUL [US]) 24 January 2002 (2002-01-24) * paragraphs [0325] - [0346]; figures 1-4 *	1-37	
A	WO 03/102726 A (ACS STATE & LOCAL SOLUTIONS IN [US]) 11 December 2003 (2003-12-11) * paragraphs [0045] - [0094]; figures 1-15 *	1-37	
A	US 2005/240613 A1 (LOGAN CARMEN JR [US] LOGAN JR CARMEN [US]) 27 October 2005 (2005-10-27) * paragraphs [0049] - [0087]; figures 1-22 *	1-37	
			TECHNICAL FIELDS SEARCHED (IPC) G06F G06Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	24 October 2007	SCHECHNER-RESOM, M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 07 10 7865

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

24-10-2007

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6117073 A	12-09-2000	NONE	
US 2002010679 A1	24-01-2002	NONE	
WO 03102726 A	11-12-2003	AU 2003229090 A1	19-12-2003
US 2005240613 A1	27-10-2005	US 2006206361 A1	14-09-2006

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 6117073 A **[0019]**